

CompTIA

Security+

SY0-201 SY0-201 SY0-201 SY0-201 SY0-201 SY0-201 **SY0-201**

PRINTABLES

PRINTABLE PRACTICE QUESTIONS

QUESTIONS, ANSWERS, AND
DETAILED EXPLANATIONS IN AN
EASY-TO-USE PRINTABLE FORMAT

PrepLogic

Be Prepared. Be Confident. Get Certified.

Chapter 1

Systems Security

1. Which of the following are reasons why you should be concerned with email spam? Select the best answers.
- A. It violates US federal law.
 - B. It threatens physical server room security.
 - C. It blocks Internet access.
 - D. It consumes computer and network resources.

[Find the Answer](#) p. 135

2. What is the single largest issue preventing widespread adoption of Instant Messaging (IM)? Select the best answer.
- A. Concerns regarding lower work productivity.
 - B. A lack of standards between IM vendors.
 - C. There is no standardization.
 - D. No native support of encryption.

[Find the Answer](#) p. 135

3. When would a cookie be a security issue? Select the best answer.
- A. When the cookie stores credit information.
 - B. When it's a "magic cookie".
 - C. When it becomes deleted.
 - D. Cookies are never a security issue.

[Find the Answer](#) p. 135



4. What is the purpose of a Simple Mail Transfer Protocol (SMTP) relay? Select the best answer.
- A. To accept connections from users, usually at a different location from the server, who wish to receive email.
 - B. To accept connections from users, usually at a different location from the server, who wish to send email.
 - C. To accept connections from users, usually at a different location from the server, who wish to send cookies.
 - D. To accept connections from users, usually at a different location from the server, who wish to receive cookies.

[Find the Answer](#) p. 135

5. Besides cleartext visibility, what other issues are involved with the usage of Instant Messaging (IM) applications in the workplace? Select the best answer.
- A. Port
 - B. Protocol
 - C. Policy
 - D. Procedure

[Find the Answer](#) p. 135

6. Success with firewalls and email require allowing certain ports to pass traffic. From the answer choices provided, select the correct port configuration. Select the best answer.
- A. SMTP port 110, POP3 TCP port 80, IMAP TCP 143
 - B. SMTP port 25, POP3 port 110, IMAP TCP 143
 - C. SMTP port 25, POP3 UDP port 143, IMAP TCP 80
 - D. SMTP port 110, POP3 TCP port 143, IMAP TCP 25

[Find the Answer](#) p. 135



Answers: Chapter 1

1. A, D	Review Question p. 2	Detailed Explanation p. 154
2. D	Review Question p. 2	Detailed Explanation p. 154
3. A	Review Question p. 2	Detailed Explanation p. 154
4. B	Review Question p. 3	Detailed Explanation p. 155
5. C	Review Question p. 3	Detailed Explanation p. 155
6. B	Review Question p. 3	Detailed Explanation p. 156
7. D	Review Question p. 4	Detailed Explanation p. 156
8. B	Review Question p. 4	Detailed Explanation p. 157
9. C	Review Question p. 4	Detailed Explanation p. 157
10. C	Review Question p. 5	Detailed Explanation p. 157
11. B	Review Question p. 5	Detailed Explanation p. 158
12. C	Review Question p. 5	Detailed Explanation p. 158
13. A	Review Question p. 6	Detailed Explanation p. 159
14. B	Review Question p. 6	Detailed Explanation p. 159
15. C	Review Question p. 6	Detailed Explanation p. 159
16. D	Review Question p. 7	Detailed Explanation p. 160
17. D	Review Question p. 7	Detailed Explanation p. 160
18. C	Review Question p. 7	Detailed Explanation p. 161
19. C	Review Question p. 8	Detailed Explanation p. 161
20. C	Review Question p. 8	Detailed Explanation p. 162
21. B	Review Question p. 8	Detailed Explanation p. 162
22. B	Review Question p. 9	Detailed Explanation p. 162
23. D	Review Question p. 9	Detailed Explanation p. 163



Explanations: Chapter 1

1. [Review Question](#) p. 2

Answers: A, D

Explanation A. Correct. Select forms of spam are federally regulated under the Can-spam bill. Consequently, many such offenders outsource operations to other countries where no such laws regulate spam.

Explanation B. Incorrect. Server room physical security would be affected by direct, not wire-borne threats to your servers. Spam may carry viruses, but these do not pose a threat to server room physical security.

Explanation C. Incorrect. Spam does not directly block Internet access, but it can significantly slow network performance and complicate email reception.

Explanation D. Correct. You could argue that if you get enough spam, your network could conceivably crash and your users would not be able to access the Internet.

PrepLogic Question: [11344-1049](#)

2. [Review Question](#) p. 2

Answers: D

Explanation A. Incorrect. Some businesses are interested in using IM because it can stimulate work productivity through collaboration.

Explanation B. Incorrect. Since a business is typically a single unit, a lack of standards between different IM offerings is a low priority, as all a business needs to do is pick one vendor, company wide.

Explanation C. Incorrect. Despite the fact there are nearly as many IM protocols as there are IM clients, this is not a significant hindrance for multi-protocol platforms or business.

Explanation D. Correct. IM originated as a personal application for two-way communications between individuals. As is the case with many protocols, few IM protocols and platforms provide any native encryption capability.

PrepLogic Question: [11344-1052](#)

3. [Review Question](#) p. 2

Answers: A



Explanation A. Correct. Cookies store data in a plain text format. Cookies can only contain information that was provided by the user to the web server.

Explanation B. Incorrect. Magic cookies and a web server work with unique data (user's email address or a "magic number" understood by the web server). This data is matched with page requests to give the web session a "state" that can help track where the user has been on the web site.

Explanation C. Incorrect. A cookie cannot reveal data when it is deleted, so deleting a cookie does not present a security issue.

Explanation D. Incorrect. Cookies store data in a plain text format. Cookies can only contain information that was provided by the user to the web server.

PrepLogic Question: [11344-1056](#)

4. [Review Question](#) p. 3

Answers: B

Explanation A. Incorrect. This is the correct purpose, but the wrong direction. Remember, it is far more common to use POP3 (Post Office Protocol) to receive email.

Explanation B. Correct. SMTP relays accept connections from users who wish to send emails.

Explanation C. Incorrect. Cookies have nothing to do with SMTP. Remember what SMTP stands for.

Explanation D. Incorrect. Cookies have nothing to do with SMTP. Remember what SMTP stands for.

PrepLogic Question: [11344-1061](#)

5. [Review Question](#) p. 3

Answers: C

Explanation A. Incorrect. Many IM platforms establish outbound port-bound connections, which aren't a problem for firewalls (unless expressly prohibited) or intrusion detection systems (IDS).

Explanation B. Incorrect. Some IM platforms use standardized protocols and others utilize their own proprietary protocols, but neither presents a significant issue for firewall and intrusion detection systems (IDS).



Explanation C. Correct. Instant messaging, like email, may be regulated by company or federal compliance policies. This can be prohibitive in certain working environments where strict regulatory practices and policies forbid IM applications.

Explanation D. Incorrect. There is nothing procedurally prohibitive about using IM platforms in the workplace.

PrepLogic Question: [11344-1068](#)

6. [Review Question](#) p. 3

Answers: B

Explanation A. Incorrect. These are not correct port numbers. A portion of your knowledge being tested is 'knowing the numbers', as this question illustrates.

Explanation B. Correct. Port number assignment can vary to accommodate various needs. When communicating with other systems, though, standards must be followed and firewalls need to allow the appropriate traffic through.

Explanation C. Incorrect. These are not correct port numbers. A portion of your knowledge being tested is 'knowing the numbers', as this question illustrates.

Explanation D. Incorrect. These are not correct port numbers. A portion of your knowledge being tested is 'knowing the numbers', as this question illustrates.

PrepLogic Question: [11344-1069](#)

7. [Review Question](#) p. 4

Answers: D

Explanation A. Incorrect. A virus infects a computer and requires a host (file) to be manually accessed for propagation to occur.

Explanation B. Incorrect. A worm is similar to a virus except that it propagates automatically, requiring no intervention.

Explanation C. Incorrect. A Trojan horse often consists of two parts: 1) an actual program that has a legitimate use; and 2) the Trojan itself, which is the part that maliciously functions in the background.

Explanation D. Correct. A logic bomb is a piece of malicious code that may remain dormant until a particular event or sequence of events occurs.

PrepLogic Question: [11344-1096](#)

